UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/030,318	04/12/2002	Thomas E Rowley III	P400749	5771

46155 7590 08/08/2007

ALEXANDER R SCHLEE
SCHLEE IP INTERNATIONAL P.C.
3770 HIGHLAND AVENUE, SUITE 203
MANHATTAN BEACH, CA 90266

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
08/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/030,318	ROWLEY, THOMAS E	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on August 16, 2006. Claims 1 – 14 were amended and new claims 15 – 18 were added. Claims 1 – 18 are pending.

Specification

2. Amendment to abstract and title has been noted and entered. Cross reference to related applications has been updated.

Information Disclosure Statement

3. The listing of references in the specification is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, or other information submitted for consideration by the Office, and MPEP § 609.04(a) states, "the list may not be incorporated into the specification but must be submitted in a separate paper." Therefore, unless the references have been cited by the examiner on form PTO-892, they have not been considered.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., In re Berg, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir.

1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 1 – 18 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 – 22 of U.S. Patent No. 5,991,408. Although the conflicting claims are not identical, they are not patentably distinct from each other because in the instant case all elements of claims 1 – 18 correspond to claims 1 – 22 of the patent, except in the instant claims recite "a plurality of templates representing enrolled biometric information, a biometric public key private key pair corresponding to each of said plurality of templates" is referred in claims of the patent as "representing biometric features in the plurality of biometric features and determining a cryptographic key". It would have been obvious to one having ordinary skill in the art to recognize that the public/private key is equivalent to the cryptographic key.

Claims of the instant application therefore are not patentably distinct from the earlier patent claims and as such are unpatentable for obvious-type double patenting (*In re Goodman (CAFC) 29 USPQ2d 2110 12/3/1993).*

Response to Arguments

5. Applicant's arguments filed on 8/16/2006 have been fully considered.

5.1 Applicant argues that "further comprising steps performed by said host computer, said steps comprising:" or "further comprising steps performed by a remote computer, said steps comprising:" is not objectionable. Examiner points the claims language "further comprising steps performed by said host computer, said steps comprising:" does not clearly point out that Claim 8 or Claim 9 is further narrowing the limitations of Claim7 or Claim 8.

Examiner respectfully maintains previous objections. Applicant is advised to amend the claims as suggested before or amend the claims to overcome language objections.

With respect to Claim numbering, Examiner notes the order of Claim numbers are proper with the amended claims and withdraws objections for Claims 10 – 14.

5.2 Applicant argues that the Claims 1-5 and 11-14 do not violate the written description requirement because the subject matter is fully supported in the disclosure and cites specification page 17 lines 21 – 24 for "the trusted sensor includes a public key and private key pair for each biometric template ... stored in the trusted sensor".

Examiner agrees with the Applicant and withdraws the rejection. However, please also refer to section **5.3** and **6** below.

5.3 Applicant agrees with the Examiner that "a secure communication link" is not disclosed in the specifications **but has not** amended the claim. Examiner maintains the rejection (see section **7** below).

5.4 Applicant argues that Bjorn does not disclose "a biometric public key private key pair corresponding to each of said plurality of templates" and does not disclose "a cryptographic library module storing one or more public private key encryption functions"; "determining whether said biometric information from said image capture device matches an enrolled biometric template stored in said trusted sensor"; "...deny the access to the key pairs and cryptographic library module".

Referring to the previous office action, Examiner had cited relevant portions of the references as a means to illustrate the system as taught by the prior art. As a means of providing further clarification as to what is taught by the references used in the first office action, Examiner has expanded the teachings for comprehensibility while maintaining the same grounds of rejection of the claims. Examiner respectfully requests that the Applicant consider all the teachings from the cited art as well as those that are incorporated by reference.

Bjorn teaches "A sensor to obtain user's fingerprints, a security unit to encrypt and decrypt messages, a comparator for comparing fingerprint data and a storage unit to store fingerprint templates, identification data for each individual person who is registered in the system" (See Column 3 line 22 – Column 7 line 31). Furthermore, Bjorn teaches "a cryptographic generation using biometric data", which is disclosed in

patent 6,035,398 (Ser.No. 08/970,304), which is incorporated by reference (please refer to Column 6 liens 45 – 51). Examiner maintains prior art rejection.

Examiner suggests applicant to amend the claims in a manner to distinct applicant's invention with prior art with ***attention*** given to the amended specification page 19 line 1 – page 20 line 14).

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6 Claims 1 – 18 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claims 1 – 18 recite "biometric public key private key pair", which is not disclosed in the instant specification.

Examiner points to page 17 from lines 25 onward, **as an example**, to the disclosed subject matter which reads, "Now turning to FIG. 4, which depicts the enrollments process .... Next, a public key 28 private key 30 pair is generated for the captured biometric information". Examiner requests the applicant to amend the claims to reflect such public/private key pair to be generated for the particularly captured

biometric information and also **emphasize** that such public/private key pair is not a biometric public/private key pair but generated **for** each biometric information.

7. Claim 5 recites "a peripheral interface (50) configured .... over a secure communication link (16)".

With respect to "a secure communication link (16)", even though instant specification discloses "The host computer 12 is connected to a trusted sensor 14 by a data transfer bus 16, e.g., a standard RS-232 or a Universal Serial Bus ("USB") serial data interface bus" (see instant application amended page 11 lines 26 – 28) and "The functions section 32 includes a peripheral interface 50 to the host computer 12 over the bus 16, which may be a serial interface such as an RS-232, USB or a bus level bus like ISA, or PCI, with the preferred embodiment comprising an ISA interface (see instant application amended page 13 lines 1 – 3), the specification does not disclose "a secure communication link".

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claims 1 – 18 are rejected under 35 U.S.C. 102(e) as being anticipated by Bjorn et al. (U.S. Patent Number 6,122,737).

Regarding Claims 1 and 18, Bjorn teaches a microprocessor; a data memory coupled to said microprocessor and configured to hold a plurality of templates representing enrolled biometric information, a biometric public key private key pair corresponding to each of said plurality of templates, and a manufacturer public key and private key pair (Column 4 lines 21 – 25); and

a functions section coupled to said microprocessor, said functions section comprising:

a cryptographic library module storing one or more public key private key encryption functions and further storing instructions for causing said microprocessor to populate said biometric public key and private key pair corresponding to each of said plurality of templates (Column 4 lines 44 – 47);

a feature extraction and template matching module storing instructions for causing said microprocessor to extract features created with a biometric image capture device coupled to said trusted sensor and to populate to at least one of said plurality of templates, and further storing instructions for causing said microprocessor to match sensed biometric information, communicated from said biometric image capture device, to said enrolled biometric information stored said data memory and, based on said match, select a particular biometric private key (Column 4 lines 44 – 62); and

an authentication module storing instructions for causing said microprocessor to certify said trusted sensor to a host computer by executing said one or more encryption functions stored in said cryptographic module using said manufacture private key and a host computer public key (Column 4 lines 44 – 62).

Regarding Claim 6, Bjorn teaches performing a power on self-test on said trusted sensor; verifying said on said trusted sensor to a host computer coupled to said trusted sensor, said step of verifying using a manufacturer private key and a host computer public key (Column 4 lines 44 – 47);

receiving biometric information from an image capture device; matching said biometric information from said image capture device to an enrolled biometric template stored in said trusted sensor (Column 4 lines 44 – 47);

selecting a public key and a private key pair corresponding to said enrolled biometric template, said public key and private key pair stored in said trusted sensor (Column 4 lines 44 – 47);

receiving a message from said host computer, said message including a remote computer public key; encrypting at least a portion of said message using said selected private key and said remote computer public key; and sending said encrypted message form said trusted sensor to said host computer (Column 3 lines 37 – 56 and Column 4 lines 44 – 47).

Regarding Claim 11, Bjorn teaches a remote computer including a remote computer public key and private key pair; a host computer coupled to said remote computer, said host computer including a host computer public key and private key pair (Column 4 lines 44 – 47 and Column 5 lines 2 – 15);

a biometric image sensing means including a plurality of capacitive sensing elements for measuring relative distances between ridges and valleys on a fingerprint (Column 4 lines 44 – 47); and

a trusted sensor coupled to said biometric image sensing means and said host computer, said trusted sensor including a microprocessor, a functions section accessible by said microprocessor, and a data memory including a plurality of biometric templates, each of said plurality of biometric templates having a biometric template public key and private key pair, and a manufacturer public key and private key pair, wherein biometric information sensed by said biometric image sensing means is manipulated and stored in said plurality of biometric templates, and wherein each of said biometric template public key and private key pairs is dependent upon said manipulated biometric information stored in corresponding one of said plurality of biometric templates(Column 3 lines 37 – 56; Column 4 lines 44 – 47 and Column 5 lines 1 – 40).

Claim 2 is rejected applied as above in rejecting Claim 1. Furthermore, Bjorn teaches authentication module further storing instructions for causing said microprocessor to execute said one or more encryption functions stored in said cryptographic library module using said particular biometric private key, a public key corresponding to a remote computer, said one or more encryption functions encrypting a message destined for said remote computer (Column 3 lines 37 – 56; Column 4 lines 44 – 47 and Column 5 lines 1 – 40).

Claim 3 is rejected applied as above in rejecting Claims 1 – 2. Furthermore, Bjorn teaches wherein said biometric image capture device includes a plurality of capacitive fingerprint sensing elements; and

wherein said manufacturer public key and private key pair correspond to said plurality of capacitive fingerprint sensing elements (Column 3 lines 37 – 56; Column 4 lines 44 – 47 and Column 5 lines 1 – 40).

Claim 4 is rejected applied as above in rejecting Claims 1 – 2. Furthermore, Bjorn teaches wherein said biometric image capture device includes a plurality of capacitive fingerprint sensing elements; and

wherein said manufacturer public key and private key pair correspond to said functions section (Column 3 lines 37 – 56; Column 4 lines 44 – 47 and Column 5 lines 1 – 40).

Claim 5 rejected applied as above in rejecting Claims 1 – 3. Furthermore, Bjorn teaches said functions section further comprising:

a power on self-test and tamper detect feature storing instructions for causing said microprocessor to enable said trusted sensor when said power on self-test is successful and said tamper detected feature detects no tampering (Column 4 lines 44 – 47);

a secure time stamp module storing instructions for causing said microprocessor to generate a time stamp used by said authentication module; and a peripheral interface

configured to communicatively couple microprocessor to said host computer over a secure communications link (Column 7 lines 11 – 18).

Claims 7 and 15 are rejected applied as above in rejecting Claims 6 and 10. Furthermore, Bjorn teaches said step of verifying comprising:

receiving an encrypted random number from said host computer, said encrypted random number encrypted by said host computer using a host computer private key and a manufacturer public key (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

decrypting said encrypted random number into a random number using said host computer public key and said manufacturer private key (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

modifying said random number; encrypting said modified random number using said manufacturer private key and said host computer public key; and sending said encrypted modified random number to said host computer (Column 5 lines 25 – 32 and Column 6 lines 45 – 63).

Claims 8 and 16 are rejected applied as above in rejecting Claims 6 – 7 and Claim 15. Furthermore, Bjorn teaches steps performed by said host computer, said steps comprising:

generating said random number; encrypting said random number using said host computer private key and said manufacturer public key to form said encrypted

random number; sending said encrypted random number to said trusted sensor (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

receiving said encrypted modified random number from said trusted sensor; decrypting said encrypted modified random number using said host computer private key and said manufacturer public key; and verifying said modification performed by said trusted sensor to said random number (Column 5 lines 25 – 32 and Column 6 lines 45 – 63).

Claims 9 and 17 are rejected applied as above in rejecting Claims 6 – 8 and Claim 16. Furthermore, Bjorn teaches further comprising steps performed by said remote computer, said steps comprising:

encrypting a primary message with a remote computer private key and a transaction public key, said transaction public key selected from a group comprising said host computer public key (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

receiving a confirmation message from said host computer, said confirmation message comprising said portion of said message encrypted at said trusted sensor using said selected private key and said remote computer public key (Column 5 lines 25 – 32 and Column 6 lines 45 – 63); and

decrypting said portion of said confirmation message using said selected transaction key and said remote computer private key (Column 5 lines 25 – 32 and Column 6 lines 45 – 63).

Claim 10 is rejected applied as above in rejecting Claims 6 – 9. Furthermore, Bjorn teaches one or more computer readable mediums having stored therein one or more sequences of instructions for causing one or more microprocessors to perform the steps (Column 3 line 63 – Column 4 line 4).

Claim 12 rejected applied as above in rejecting Claims 6 – 10. Furthermore, Bjorn teaches wherein said trusted sensor is verified by host computer by:

sending a first message from said host computer (12) to said trusted sensor (14), said first message encrypted with said host computer private key (44) and said manufacturer public key (38) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

receiving said first message at said trusted sensor, decrypting said first message, manipulating a portion of said first message, returning a return first message to said host computer, said return first message including said manipulated portion of said first message and said return first message encrypted with said manufacturer private key and said host computer public key (Column 5 lines 25 – 32 and Column 6 lines 45 – 63); and

receiving said return first message from said trusted sensor at said host computer, decrypting said return first message with said host computer private key and said manufacturer public key and verifying said manipulation to said portion of said first message (Column 5 lines 25 – 32 and Column 6 lines 45 – 63).

Claim 13 is rejected applied as above in rejecting Claims 6 – 12. Furthermore, Bjorn teaches wherein a transaction is verified, after first verifying said trusted sensor, by: sensing current user biometric information using said biometric image sensing means; comparing said current user biometric information to said plurality of biometric templates (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

selecting a particular biometric image template that matches said current user biometric information, said act of selecting including identifying a particular biometric public key and private key pair corresponding to said particular biometric image template (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

encrypting a second message authorizing a transaction with said particular biometric private key and said remote computer public key; sending said second message to said host computer (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

receiving said second message from said trusted sensor at said host computer; re-transmitting said second message from host computer to said remote computer (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

receiving said re-transmitted second message from host computer at said remote computer; and verifying said re-transmitted second message using said host computer private key and said particular biometric public key (Column 5 lines 25 – 32 and Column 6 lines 45 – 63).

Claim 14 is rejected applied as above in rejecting Claim 13. Furthermore, Bjorn teaches wherein prior to said step of re-transmitting said second message, and host computer encrypts said second message using said host computer private key and said remote computer public key (Column 5 lines 25 – 32 and Column 6 lines 45 – 63); and

wherein said step of verifying said re-transmitted second message includes verifying said second message using said host computer public key (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-232-4195. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
July 30, 2007.